CLAIMS

What is claimed is:

1. A method for creating an apparatus for securely providing identification information comprising:

generating a visual filtering pattern that when combined with a displayed obscured user identifier, visually reveals an identifier; and

generating a translucent identification member having the visual filtering pattern thereon.

2. The method of claim 1 including:

assigning identification information to the visual filtering pattern;

storing the identification information and associated visual filtering pattern; and

providing the identification information on the translucent identification member.

3. An apparatus for creating an apparatus for securely providing identification information comprising:

an issuer operative to generate a visual filtering pattern that when combined with a displayed obscured user identifier, visually reveals an identifier; and operative to generate a translucent identification member having the visual filtering pattern thereon.

4. The apparatus of claim 3 wherein the issuer is operative to assign identification information to the visual filtering pattern; store the identification information and associated visual filtering pattern; and provide the identification information for placement on the translucent identification member.

5. An apparatus for creating an apparatus for securely providing identification information comprising:

a translucent identification member issuer operative to generate a translucent identification member having a translucent area that includes a visual filtering pattern thereon configured to visually filter a displayed obscured unique identifier and configured to overlay at least a portion of a display screen.

6. A method for securely providing identification information comprising:

sending a pattern containing one or more obscured user identifiers wherein the pattern of obscured user identifiers is defined such that when a visual filtering pattern contained on a translucent identification member is combined with the one or more obscured user identifiers located in the pattern, a designated one of the one or more obscured user identifiers is revealed; and

receiving data representing the revealed identifier.

7. The method of claim 6 wherein the pattern is sent to a display device.

8. The method of claim 6 including sending the received data representing the revealed expected identifier to an authentication apparatus.

9. A method for securely providing identification information comprising:

receiving user identification information as a first factor of authentication for a user;

using such user identification information to identify a translucent identification member containing a particular visual filtering pattern known to have been associated with such user;

generating an expected identifier to be used as a second factor of authentication for the user associated with the received user identification information;

generating a pattern of one or more obscured user identifiers containing the expected identifier such that when the pattern of obscured user identifiers is combined with the visual filtering pattern on the identified translucent identification member associated with the user the expected identifier will be revealed;

transmitting the pattern of obscured user identifiers to a display and requesting entry of a revealed identifier; and

receiving data representing the revealed identifier.

10. The method of claim 9 including examining the received data representing the revealed identifier to determine if it matches the expected identifier.

11. The method of claim 10 wherein the expected identifier has been determined before receipt of the received data representing the revealed identifier.

12. The method of claim 10 wherein the expected identifier is determined after receipt of the received data representing the revealed identifier.

13. The method of claim 10 including granting a right to the user if the received data representing the revealed identifier matches the expected identifier.

14. The method of claim 10 wherein examining the received data representing the revealed identifier is done by sending the received data to an authentication apparatus.

15. The method of claim 14 including receiving a reply from the authentication apparatus and granting a right to the user if the authentication apparatus indicates that a match with the expected identifier occurred.

16. The method of claim 9 wherein the step of using the user identification information includes checking if the translucent identification member is valid based on a list of invalid translucent identification members.

17 A method for associating secure identification information with a user comprising:

receiving a request from a user for a filtering pattern; and

recording a link between the user and the identification information associated with the filtering pattern.

18. The method of claim 17 including providing the filtering pattern to the user.

19. The method of claim 18 wherein the filtering pattern is on a translucent identification member that is sent to the user.

20. The method of claim 18 wherein the filtering pattern is sent to a third party to be placed on a translucent identification member for the user.

21. The method of claim 18 wherein the filtering pattern is sent to the user for placement on a translucent identification member.

22. The method of claim 17 wherein the filtering pattern is selected from a pre-existing pool of filtering patterns.

23. The method of claim 17 wherein the request from the user includes user specific information and wherein the user specific information is combined with other information to produce the filtering pattern.

24. The method of claim 17 wherein the request from the user includes user specific information and wherein the user specific information is used to produce the filtering pattern.

25. A method for securely providing identification information comprising:

generating at least one visually obscured user identifier for display on a display; and

sending the generated visually obscured user identifier for display in response to a recipient unit request.

26. The method of claim 25 wherein generating the at least one visually obscured user identifier includes obtaining user specific information associated with a user; and

combining the user specific information with other information to produce the at least one visually obscured user identifier.

27. The method of claim 25 wherein the at least one visually obscured user identifier is generated independent from user specific information.

28. A system for securely providing identification information comprising:

a circuit operative to receive user identification information as a first factor of authentication for a user;

a circuit operative to use such user identification information to identify a translucent identification member with a particular visual filtering pattern known to have been associated with such user;

a circuit for generating an expected identifier to be used as a second factor of authentication for the user associated with the received user identification information;

a circuit for generating an pattern of one or more obscured user identifiers containing the expected identifier such that when the pattern of obscured user identifiers is combined with the visual filtering pattern on the identified translucent identification member associated with the user the expected identifier will be revealed;

a circuit for transmitting the pattern of obscured user identifiers and for requesting entry of a revealed identifier; and

a circuit for receiving data representing the revealed identifier.

29. The system of claim 28 including a circuit to examine the received data representing the revealed identifier to determine if it matches the expected identifier.

30. The system of claim 29 wherein the circuit for examining the received data can determine the expected revealed identifier prior to receipt of the received data representing the revealed identifier.

31. The system of claim 29 wherein the circuit for examining the received data can determine the expected revealed identifier after receipt of the received data representing the revealed identifier.

32. The system of claim 29 including a circuit to grant a right to the user if the received data representing the revealed identifier matches the expected revealed identifier.

33. An apparatus for securely providing identification information comprising:

a translucent identification member authenticator operative to receive data from a user representing a revealed identifier in response to overlaying a translucent identification member containing a visual filter on a display; and operative to compare the received data with a corresponding expected identifier to determine whether proper authentication of the user is appropriate.

34. The apparatus of claim 33 wherein the translucent identification member authenticator determines the expected revealed identifier prior to the receipt of the received data corresponding to the revealed identifier.

35. The apparatus of claim 33 wherein the translucent identification member authenticator determines the expected revealed identifier after the receipt of the received data corresponding to the revealed identifier.

36. An apparatus for associating secure identification information with a user comprising:

a circuit operative to receive a request from a user for a filtering pattern; and operative to record a link between the user and the identification information associated with the filtering pattern.

37. The apparatus of claim 36 wherein the circuit is operative to select the filtering pattern is selected from a pre-existing pool of filtering patterns.

38. The apparatus of claim 36 wherein the circuit is operative to request information from the user that includes user specific information and wherein the user specific information is combined with other information to produce the filtering pattern.

39. The apparatus of claim 36 wherein the circuit is operative to request information from the user that includes user specific information and wherein the user specific information is used to produce the filtering pattern.

40. An apparatus for securely providing identification information comprising:

a translucent identification member authenticator operative to receive data representing a revealed identifier from the displayed obscured user identifier, in response to an overlaying of a translucent identification member having a visual filtering pattern thereon on the display; and operative to send the data representing the revealed identifier for comparison with a corresponding expected identifier to determine whether proper authentication of a recipient is appropriate.

41. The apparatus of claim 40 including an obscured user identifier generator operative to generate at least one visually obscured user identifier for display on a display, in response to received user information.

42. An apparatus for securely providing identification information comprising:

a translucent identification member authenticator operative to receive data representing a revealed identifier from the displayed obscured user identifier, in response to an overlaying of a translucent identification member having a visual filtering pattern thereon on a display; and operative to compare the received revealed identifier with a corresponding expected identifier to determine whether proper authentication of a user is appropriate.

43. The apparatus of claim 42 wherein the translucent identification member authenticator is operative to send right grant information to a user unit in response to the received data matching the corresponding expected identifier.

44. A method for securely providing identification information comprising:

displaying at least one visually obscured user identifier as user authentication data; and

receiving data representing revealed user authentication data that is derived when a translucent identification member having a filtering pattern thereon is combined therewith.

45. The method of claim 44 including receiving user specific information, prior to the step of displaying the obscured user identifier, to determine the at least one revealed user authentication data.

46. The method of claim 44 wherein the data representing the revealed user authentication data is received using a device other than the device that was used to display the obscured user identifier.

47. An apparatus for securely providing identification information comprising:

a display circuit operative to display one or more obscured user identifiers defined such that when the one or more obscured user identifiers are combined with a filtering pattern

located on a translucent identification member, a designated one of the one or more obscured user identifiers is revealed; and

an input interface operative to receive data representing the revealed identifier.

48. The apparatus of claim 47 including a transmission circuit operative to transmit the received data representing the revealed identifier.

49. The apparatus of claim 47 wherein the interface is operative to request entry of user identification information.

50. A secure identification information member comprising:

a translucent area having a visual filtering pattern thereon configured to visually filter a displayed obscured user identifier and configured to overlay at least a portion of a display screen.

51. A transaction card comprising:

a first portion at least containing a transaction card identification information; and

a second portion containing a translucent identification member having a translucent area that includes a filtering pattern.

52. The transaction card of claim 51 wherein the second portion containing the translucent identification member includes an attached translucent identification member.

53. The transaction card of claim 51 wherein the second portion containing the translucent identification member includes an open area with a connecting structure configured to receive and hold the translucent identification member.

54. The transaction card of claim 51 wherein the translucent identification member is configured to overlay at least a portion of a display screen.